CLAIMS

1. A cross-platform single sign-on system for sharing user data across computers on a plurality of computing platforms, the system comprising:

an authentication module for authenticating a user at the beginning of a computing session;

an interface module configured to receive requests for authentication and non-authentication data associated with the user from a plurality of applications on the plurality of computing platforms and, based upon authentication of the user at the beginning of the computing session and responsive to the requests, to automatically provide authentication and non-authentication data to the plurality of applications throughout the computing session; and

a data registry in communication with the interface module for storing and providing authentication data and non-authentication data responsive to requests made by the plurality of applications.

2. The cross-platform single sign-on system of claim 1, wherein web services technologies are used to transmit requests for authentication and non-authentication data from a plurality of computer systems hosting the plurality of applications to the interface module.

3. The cross-platform single sign-on system of claim 1, wherein the non-authentication data includes state information reflecting a state of a selected application on a first

computer accessed by the user that can be retrieved when the selected application is being accessed from a second computer.

4. The cross-platform single sign-on system of claim 3, wherein the selected application is being accessed from a second computer by a second user.

5. The cross-platform single sign-on system of claim 1, wherein the interface module is further configured to receive requests to store authentication and non-authentication data associated with the user from a plurality of applications on a plurality of computing platforms in the computing system and, based upon authentication of a user at the beginning of a computing session and responsive to the requests, to store the data to the data registry.

6. The cross-platform single sign-on system of claim 1, wherein the interface module formats data queries to the data registry in accordance with a data exchange protocol accepted by the data registry.

7. The cross-platform single sign-on system of claim 1, wherein the data registry is further configured to receive requests for authentication and non-authentication data directly from the plurality of applications on the plurality of computing platforms, and for the requested data to be retrieved from the data registry responsive to the requests.

8. The cross-platform single sign-on system of claim 1, wherein a request to retrieve authentication and non-authentication data associated with the user is sent responsive to an event trigger activated during the user's computing session.

9. The cross-platform single sign-on system of claim 8, wherein the event trigger comprises at least one of: the authentication of a user, a user command, and the passage of a pre-determined interval of time.

10. The cross-platform single sign-on system of claim 1, wherein the interface module and authentication module are commonly hosted on a single computer.

11. The cross-platform single sign-on system of claim 1, wherein at least one of the plurality of computing platforms differs from another at least another of the plurality of computing platforms.

12. The cross-platform single sign-on system of claim 1, further comprising:

a caching module for storing non-authentication data generated by an application in the local cache of the computer hosting the application when the computer is disconnected from the computing system; and

a synchronizing module for sending non-authentication data stored in the local cache to the data registry when the computer is connected to the computing system.

13. The cross-platform single sign-on system of claim 1, wherein the authentication module is configured to detect that a user is logging on to the system for the first time, further comprising:

a verification module in communication with the data registry for verifying the identity of the user;

a password capture utility launched responsive to the successful verification of the user's identity for creating a global user id and password for the user with which the user can be logged on to the cross-platform single sign-on system, capturing user

authentication information associated with applications launched during the user's computing session, and storing the authentication information in the data registry.

14. A data registry for storing and providing data across a computing system, the data registry comprising:

a plurality of user data entries, each of the user data entries describing a unique user of an computing system comprised of a plurality of computing platforms and a plurality of applications;

a plurality of authentication entries associated with each of the user data entries for authenticating the user on the plurality of applications of the computing system; and

a plurality of non-authentication attributes and attribute entries associated with each of the user data entries in which information about a user's use of an application can be preserved.

15. The data registry of claim 14, wherein the non-authentication data includes state information for one of the plurality of applications, whereby a user may switch between a first computer and a second computer and preserve the state of a selected application accessed using the first computer when accessing the selected application from the second computer.

16. The data registry of claim 14, wherein the non-authentication data includes configuration information for one of the plurality of applications with which a user's application environment can be customized.

17. The data registry of claim 14, further comprising an interface module that receives web service requests for storing and providing data from one of the plurality of applications and, responsive to the requests, saves the data to the data registry.

18. A method of sharing data across a computing system, the method comprising:

subsequent to an initial authentication of a user, receiving requests to authenticate the authenticated user from a plurality of applications on a plurality of computing platforms being accessed by the authenticated user;

automatically authenticating the authenticated user to the plurality of applications being accessed by the authenticated user responsive to the initial authentication of the user;

receiving non-authentication data provided by a first instance of the authenticated user using an application in a first domain;

storing the non-authentication data provided by the first instance of the authenticated user using the application in the first domain;

receiving a request for non-authentication data from a second instance of the application in a second domain; and

supplying the requested non-authentication data provided by the first instance of the application in the first domain to the second instance of the application in the second domain.

19. The method of claim 18, wherein the second instance of the application in the second domain is associated with a second user.

20. The method of claim 18, further comprising:

receiving log on information from a user;

determining that the user is logging on to the computing system for the first time;

subsequent to the determination that a user is logging on to the computing system for the first time, verifying the identity of the user;

prompting the user to supply a user id and password;

providing the user id and password supplied by the user to a data registry to be stored therein;

capturing application authentication information provided by the user during the computing session;

storing the application authentication information provided by the user during the computing session in the data registry wherein the data registry is configured to store authentication and non-authentication data.

21. The method of claim 18, wherein an operating platform used by the first domain differs from an operating platform used by the second domain.

22. The method of claim 18, further comprising storing authentication data in the data registry.

23. The method of claim 18, wherein the non-authentication data provided by the first instance of the application in the first domain comprises configuration information for customizing a user's application environment.

24. The method of claim 18, wherein the non-authentication data provided by the first instance of the application in the first domain includes state information with which the user's application state from the first instance of the application in the first domain can be maintained to the second instance of the application in the second domain.

25. The method of claim 18, wherein storing the non-authentication data comprises:
configuring a non-authentication data attribute;
storing a value for the non-authentication data attribute associated with the user; and
responsive to a request identifying the non-authentication data attribute, providing the value of the non-authentication data attribute to a requesting application.

26. The method of claim 18, wherein the request for non-authentication data associated with the authenticated user is generated responsive to a call trigger.

27. The method of claim 18, wherein the step of receiving non-authentication data provided by a first instance of an application used by the authenticated user comprises receiving the non-authentication data from a synchronizing module on a computer for sending non-authentication data from the local cache of the computer, the data having been stored in the local cache when the authenticated user was disconnected from the networked system.

28. The system of claim 1, wherein the non-authentication data comprises one of: configurations data, settings data, or applications data, environment data.

29. The system of claim 1, wherein the non-authentication data comprises one of: a size of a window, the configuration of a tool bar, and the selection of open files.